

REMARKS

Receipt is acknowledged of the Office Action of July 2, 2002. Claims 1-22 are currently pending in the application. Claims 1-22 have been rejected in the Office Action. Applicants amended Claims 1, 5, 8, 11, 13, 17, 21 and 22 to more particularly claim the subject matter of the invention. No new matter has been added. Favorable reconsideration of this application as amended is respectfully requested.

The Examiner has indicated in the Office Action that a copy of U.S. Patent No. 0034847 was not provided with an Information Disclosure Statement. Applicants apologize for the oversight and respectfully submit to the Examiner that the patent document cited in the IDS is U.S. Patent Application having a Publication No. US2001/0034847A1. A copy of this reference is enclosed herewith.

In the Office Action, Claims 1, 3-7, 9-11, 13-15, 17-19 and 21-22 were rejected under 35 U.S.C. §103(a), as being unpatentable over Emigh in view of Violino and Netwon Telecom Dictionary. Applicants respectfully disagree with the Examiner as discussed further below.

As claimed in independent Claims 1, 5, 8, 11, 13, 17, 21 and 22 of the present Application, the present invention relates to a method and apparatus for monitoring the integrity and security of a computer network. The security system of the present invention monitors the integrity of an individual computer connected to a target network and/or the entire target network by having at least one security subsystem. The security subsystem is located on the network and is configured to monitor all event messages generated across the entire target network of computers. By monitoring all events on the network, the subsystem detects attacks on various

Docket No.: 881075/3

network devices regardless of where these devices are located on the network. Thus, it detects attacks on individual computers and the entire network. A master security system monitors the security subsystem through a secure link and registers information pertaining to attacks detected by the security subsystem.

The NetRanger product disclosed in the cited Emigh reference implements intrusion detection technology. NetRangers passively capture information from devices associated with them on a computer network. Similarly to the network IDS 18 shown in Fig.1 of the present application, NetRanger is monitoring a limited area of the network from a fixed point of view. Thus, if a NetRanger device is associated with an individual computer, the device can only detect events generated by this individual computer and not events generated somewhere else on the network. As is disclosed in the Electronic Commerce News reference sent by the Examiner, "NetRanger sensors are deployed at critical locations on a company's network." Such deployment of multiple sensors in several fixed locations is necessary for devices based on the intrusion detection technology because of their limited event view.

Thus, Emigh does not disclose a security subsystem or detection means configured to monitor events across the network of computers in its entirety. Likewise, Emigh does not teach monitoring events across the computer network in its entirety using the security subsystem or the detection means. Instead, Emigh teaches an intrusion detection device equivalent to the network IDS 18, shown in Fig. 18 of the present application. Moreover, none of the other references cited by the Examiner discloses a security system having a security subsystem or detection means configured to monitor events across the network of computers in its entirety, or a method for monitoring the integrity of the detection means or subsystem by, inter alia, monitoring events across the computer network in its entirety.

Docket No.: 881075/3

Therefore, the limitation of the security subsystem or detection means being "configured to monitor events across said network of computers in its entirety" (Claims 1, 5, 8, 13 and 17) and the limitation of "monitoring events across said target network in its entirety using said " security subsystem or detection means (Claims 11, 21 and 22) are not met by the prior art of record. Claims 1, 5, 8, 11, 13, 17, 21 and 22 are believed to be patentable over the cited prior art. Applicants respectfully submit that dependent Claims 2-4, 6, 7, 9, 10, 12, 14-16, and 18-20 are likewise believed to define patentable subject matter in view of their dependency upon allowable Claims 1, 5, 8, 11, 13 or 17 and, further, on their own merits.

Attached hereto is a marked-up version of the changes made to the claims by the current amendment. The attached page is captioned "Version With Markings to Show Changes Made."

It is respectfully submitted that Claims 1-22, as presented, patentably define over the prior art of record. Accordingly, this Application is believed to be in a condition for allowance. Prompt and favorable action is earnestly solicited and believed to be fully warranted.

Respectfully submitted,

Schulte Roth & Zabel LLP
Attorneys for Applicant
919 Third Avenue
New York, NY 10022
(212)756-2000

By Anna Vishev
Anna Vishev
Reg. No. 45,018

Dated: October 2, 2002
New York, NY

VERSION WITH MARKINGS TO SHOW CHANGES MADE

1. (Amended) A security system for a computer connected to a network of computers comprising:

at least one security subsystem associated with said computer, said subsystem being configured to monitor events across said network of computers in its entirety and to detect attacks on said computer;

and a secure link between said security subsystem and a master system enabling data communication therebetween; wherein

said master system monitors said security subsystem through said secure link and registers information pertaining to attacks detected by said security subsystem.

5. (Amended) A network security system for a target network of computers comprising:

at least one security subsystem associated with said target network, said subsystem being configured to monitor events across said network of computers in its entirety and to detect attacks on said network; and

a secure link between said security subsystem and a master system enabling data communication therebetween; wherein

said master system monitors said security subsystem through said secure link and registers information pertaining to the attacks detected by said security subsystem.

8. (Amended) A network security system for a target network of computers comprising:

at least one security subsystem associated with said target network and configured to monitor events across said target network in its entirety and to detect and register attacks on said target network;

a secure link for data communication between said security subsystem and said master system; and

testing means associated with said master system for generating pseudo-attacks on said target network initiated by said master system and detectable by said security subsystem;

wherein

said master system monitors said security subsystem through said secure link by comparing the pseudo-attacks generated by said testing means to the detected attacks registered by said security subsystem.

11 (Amended) A method for monitoring the integrity of a security subsystem associated with a target network of computers and configured to detect attacks on said network of computers comprising:

monitoring events across said target network in its entirety using said security subsystem;
establishing a secure link for the transfer of data between said security subsystem and a master system hierarchically independent from said security subsystem;
monitoring the status of said security subsystem through said secure link; and
registering information pertaining to the status of said security subsystem.

13. (Amended) A security system for a computer connected to a computer network comprising:

at least one detection means associated with said computer, said detection means being configured to monitor events across said computer network in its entirety and to detect an attack on said computer;

a master security system located outside said computer network; and

a secure link between said detection means and said master security system enabling data communication therebetween; wherein

said master security system monitors said detection means through said secure link and registers information pertaining to attacks detected by said detection means.

17. (Amended) A network security system for a target network of computers comprising:
at least one detection means associated with said target network, said detection means being configured to monitor events across said computer network in its entirety and to detect an attack on said network;

a master security system located outside said network; and

a secure link between said detection means and said master security system enabling data communication therebetween; wherein

said master security system monitors said detection means through said secure link and registers information pertaining to attacks detected by said detection means.

21. (Amended) A method for monitoring the integrity of a detection means associated with a computer, said computer being connected to a computer network, and configured to detect an attack on said computer, said method comprising the steps of:

monitoring events across said target network in its entirety using said detection means;

Docket No.: 881075/3

establishing a secure link for the transfer of data between said detection means and a master system hierarchically independent from said detection means; monitoring the status of said detection means through said secure link; and registering information pertaining to the status of said detection means.

22. (Amended) A method for monitoring the integrity of a detection means associated with a target network of computers and configured to detect an attack on said network of computers comprising the steps of:

monitoring events across said target network in its entirety using said detection means;
establishing a secure link for the transfer of data between said detection means and a master system hierarchically independent from said detection means; monitoring the status of said detection means through said secure link; and registering information pertaining to the status of said detection means.